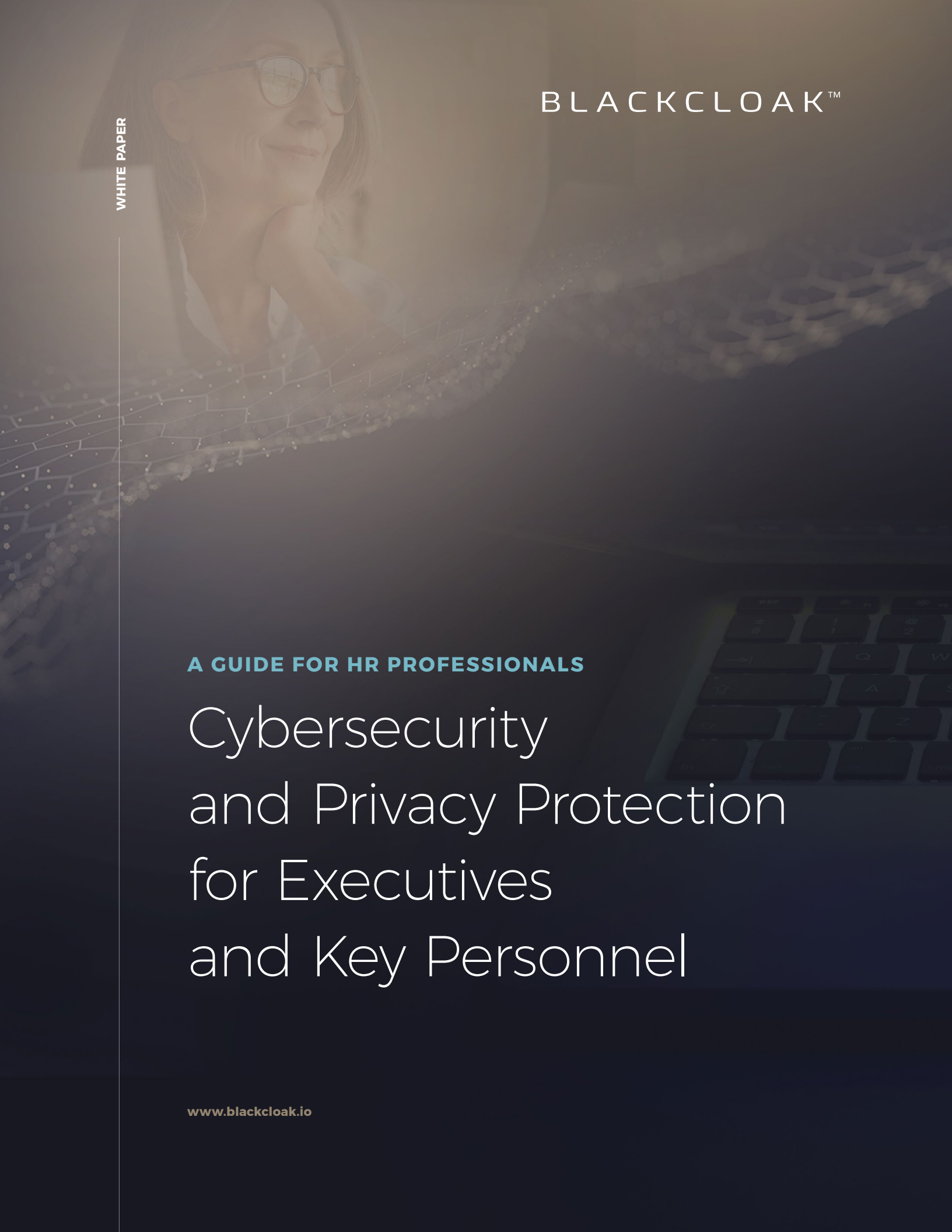


BLACKCLOAK™

WHITE PAPER

A GUIDE FOR HR PROFESSIONALS

Cybersecurity and Privacy Protection for Executives and Key Personnel

www.blackcloak.io

INTRODUCTION

> "Cybersecurity today has left the tech silo and is moving into the business front lines, where HR has a key role to play in the policy and people side of implementation."
>
> — HUMAN RESOURCE EXECUTIVE [1]

Key ideas:

The personal homes and private lives of executives are key targets for cybercriminals seeking the path of least resistance.

When it comes to executive protection, companies must balance security with privacy concerns.

HR is a key stakeholder in working with the board, the leadership team, and the CISO to make cybersecurity & privacy efforts successful for all concerned.

The business world and the office are rapidly evolving—and cyber crime is evolving, too. New technologies and software continuously create vulnerabilities while criminals are always becoming more sophisticated and innovative. According to the 2020 M-Trends report from cybersecurity company FireEye [2], 41 percent of malware deployed in 2019 was new and never seen before. Another recent report from CyberCube titled "Understanding Ransomware Trends"[3] finds organized criminals and hackers are moving away from high-volume, low-value methods of attack and switching to more sophisticated exploits that target executives and high-value individuals in their homes and private lives to gain access to corporate assets.

Alongside the need for better executive protection, boards and senior executives want to make sure their cybersecurity investment brings value and protects core business assets such as IP, customer and employee data, and reputation. Unemployment fraud targeting public-facing executives has become commonplace. And in today's social world, company reputation and the personal brand of executives has a new currency and presents a whole new risk profile.

Extending cybersecurity to protect the business means protecting an executive's identity, private life, and home. With major breaches continually exposing personal data and creating new vulnerabilities, and executives becoming a key soft target, cybersecurity isn't a quarterly topic, but an ongoing business concern. As an HR professional, you have a critical role to play alongside the CISO in building a strong business case for a cybersecurity plan that protects the business, the brand, and the people who represent it.

CYBERSECURITY AND EXECUTIVES →

CYBERSECURITY AND EXECUTIVES:

A Moving Target

Today, the threat landscape is a moving target.

It doesn't end with the office or even the executive. Cybercriminals will exploit any vulnerability, including targeting individuals and their families in the home and on the web. Mobile phones, private email accounts, connected cameras, home speakers, and social media accounts are attractive to hackers, who find home or remote environments, with more vulnerable endpoints, easier to compromise than the office. Once a cybercriminal finds an opening, this becomes the staging ground for even greater exploits.

With the rapid adoption of both business and consumer technology and connected devices, It is impossible for an individual to stay safe and secure on their own. When onboarding BlackCloak executive clients, we find that the majority are already compromised, unprotected, or exposed, creating a weak link in the overall security posture of their company.

SNAPSHOT: **THE IMPACT OF CYBER CRIME ON EXECUTIVES** →

THE IMPACT OF CYBER CRIME ON EXECUTIVES

BlackCloak Research on the State of Corporate Executives' Cybersecurity & Privacy in their Personal Lives

39%

HAD BEEN COMPROMISED (VIA HACKED COMPUTERS, CAMERAS, OR PHONES)

59%

USED NO SECURITY ON PERSONAL DEVICES (NO ANTI-VIRUS, VPN, FIREWALLS, OR PASSWORD SAFES)

69%

HAD PASSWORDS EXPOSED ON THE DEEP/DARK WEB

75%

HAD DEVICES LEAKING THEIR LOCATION AND PRIVATE DATA

THE EXECUTIVE RISK PROFILE →

THE EXECUTIVE RISK PROFILE

According to the Verizon Data Breach Investigations Report (DBIR), C-suite executives are 12 times more likely to be targeted in a cyber attack [4]. Executives are vulnerable from many angles and have a complex risk profile.

In addition to having access to sensitive data and proprietary information, an executive is the face of a company, and this alone makes them a valuable target. As personal brands and company brands intersect and define one another, there ceases to be a distinction between the two. Executives represent the business with their personal brand, and their reputations are the foundation of trust and credibility with partners, suppliers, customers and employees. If their identity is stolen or their credentials accessed, this can do considerable harm to the company as well as its partners who may also be exposed, putting strategic partnerships at risk.

Executives have very public lives. They are often active across social media and have multiple email accounts and devices. Private devices and social media accounts are vulnerable to hacking at events, at home, and while traveling. Back at home, hackers can easily gain access to cameras, game systems, smart devices, tablets, and mobile phones. They can target partners, children, and immediate contacts to gain access and information, sometimes without the knowledge of the involved party. Once a hacker has access, they exploit it to gain more information and advantage. When targeting high-profile individuals, hackers work on teams and develop sophisticated strategies for achieving their objectives. Even a small breach like taking control of a social media account can have a huge impact, especially if the hackers can use the account to expose or uncover sensitive content.

An executive's brand is also a business asset, providing value to the enterprise and establishing credibility with partners, clients, and employees. Businesses invest heavily in their executive talent. Cybersecurity and privacy protection are critical to protecting that investment. Yet cybersecurity measures often stop at the four walls of the office and cannot protect an organization's most valuable resources, their executive staff and key personnel.

Executive behavior alone cannot prevent a breach: the risk profile is too complex and technology adoption too rapid and dynamic. But even if technology were perfect, slips do occur, and cybercriminals are continually finding novel ways to surprise people into making poor choices and deploying more stealthy malware and exploits.

Executive behavior alone cannot prevent a breach: the risk profile is too complex and technology adoption too rapid and dynamic.

THE BUSINESS CASE FOR EXECUTIVE CYBERSECURITY PROTECTION →

THE BUSINESS CASE FOR EXECUTIVE CYBERSECURITY PROTECTION

Executive cybersecurity and privacy protection isn't a perk or benefit. If a criminal gains access or takes control of an executive identity or steals credentials, the risks to the business are numerous:

- **Damage to the reputation of the brand and executive**
- **Exposure of sensitive information and business intelligence**
- **Disruption of business operations and other activities**
- **Fines, financial loss and legal consequences**

Endpoint Security in a Work From Anywhere World

Today, it's easier than ever for employees to access business information systems and networks from their mobile devices and private networks. More flexible work and the hybrid office have many benefits, but the added convenience brings new risks. For executives, that risk is multiplied. While executives' corporate devices may be defended with corporate cybersecurity protection, remote environments, personal accounts, and shared family devices continually introduce other opportunities and points of entry for ambitious hackers.

Corporate security cannot intrude into an executive's private life to monitor and protect private email accounts, cameras and speakers, and other devices, including those shared or owned by family members. For effective cybersecurity protection, the line of defense must be extended to protect company assets, including key personnel with access to business information systems, in their homes and private lives. And yet today most cybersecurity measures stop short at the four walls of the office.

While overall the enterprise has hardened its on-premises security posture, measures have been slow to close this critical gap, in part because corporate monitoring of an employee's personal home and life is not a viable solution. Corporate security measures can only extend so far into an executive's private life without creating legal and ethical issues. Ultimately, cybersecurity measures that are too restrictive or intrusive create shadow IT, while ultimately undermining the organization's entire security posture.

BALANCING CONVENIENCE, SECURITY AND PRIVACY →

BALANCING CONVENIENCE, SECURITY AND PRIVACY

Executives expect privacy and ease of use.

Balancing convenience, security and privacy has been a growing concern as devices have grown lighter, smaller and faster, and the world more connected. Executives rely heavily on the convenience and ease provided by these tools, and they are consequently more exposed to the risks as well. Cybersecurity experts are increasingly recognizing that the home and private life of executives are the key battlegrounds and that rules and restrictions do not work.

Trying to police executive's actions or implementing solutions that are not easy to use will not work. Executives will simply go around those if they are not convenient or private. So, how do businesses protect their assets while defending the executive but still respecting the need for convenience and privacy?

Third-party service providers can fill the gap with concierge cybersecurity and privacy services. This solution allows businesses to put enterprise-grade cybersecurity protection around executives and key individuals while protecting their confidentiality and private data. A trusted third party can work for the business, while providing confidential, white-glove, concierge service to the executives and their staff.

> "Organizations need to ensure that technological controls are in place rather than expecting executives to operate in a secure manner."
>
> *– CIO MAGAZINE* [5]

Executive Protection: A Critical Company Need

Executive protection has traditionally been a service provided by businesses to protect high-value individuals who face physical threats or travel to risky locations. But when the risks are digital, sometimes it is not as clear where the danger lies. In today's world, value no longer exists in tangible assets but in information, ideas, IP, and people. How well businesses can protect those assets is a matter of survival over the long term.

Businesses need a plan to protect high-profile executives, board members, and key personnel when they are outside corporate walls and most vulnerable. This is even more urgent now that so much work is taking place outside the office.

In our highly connected, rapidly digitized world, executive cybersecurity and privacy protection is an essential service. While it confers secondary benefits on the executive by defending their privacy and guarding their reputation online, corporate executive protection is primarily about defending and safeguarding the business from risks.

The privacy of individuals is guaranteed and personal information is kept private. This drives compliance and keeps both the company and the individual secure.

The Cost of a Breach is Difficult to Predict

Cybersecurity professionals know better than anyone the truth in the saying "an ounce of prevention is worth a pound of cure." It is difficult to anticipate the potential fallout from a significant breach or to repair the damage done to reputation if sensitive information becomes public. In the case of ransomware, there can be a financial hit as well if the company decides to pay it to prevent public disclosure and reputation damage.

There is also another important consideration: safeguarding client and user data and privacy, which can be exposed when business systems and records are accessed on personal devices and private networks. These breaches can be costly and bring hefty fines as legislation such as General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) continue to shape consumer privacy standards and expectations.

With cybersecurity, prevention is the best protection. And today, as cybersecurity moves from its tech silo into the business front lines, Human Resources has a pivotal role to play in its success. As an owner of both company culture and workplace safety, and with expertise in both people and policy, HR is needed to help cybersecurity solutions succeed.

HR IS... →

HR IS...

A key stakeholder in implementing an effective cybersecurity strategy and culture

From candidacy to onboarding and then through changing roles over time, Human Resources essentially owns the employee journey from beginning to end.

HR transmits culture throughout the organization, granting access and system privileges and introducing and enforcing company policy. With an interest in protecting both the business and the employee, HR has a critical role to play in implementing an effective cybersecurity culture and practice. Besides their people expertise, HR has a strong understanding of policy and compliance, and how to establish effective practices and habits. Both workplace safety and compliance with laws and regulations are a key concern of HR.

Because of their insight and close relationship to people and policy, HR is a natural partner to the CISO...from advocating for the executives and ensuring compliance, to working with the team to make sure the solution is people-focused and not just technology-focused.

In the *Human Resource Executive*, Frederick Scholl, Cybersecurity Program Director at Quinnipiac University, calls for HR to become a key stakeholder in crafting cybersecurity policy and driving better culture:

> "I believe any cultural change must be supported by a strong partnership involving HR and the CISO."

He goes on to say that he is always optimistic when HR is involved. In contrast, "the absence of HR means the project will focus on security technology and miss positively impacting security culture." [1]

Working alongside the CISO, Protecting People

Today humans are at the center of any effective cybersecurity strategy, and because the executive staff is most vulnerable in their homes and personal lives, the shield of protection must extend beyond the four walls of the office to protect executives and their staff in their homes and private lives. HR is a critical liaison bringing together people and policy with technology and process. Ensuring compliance means crafting policies that do not limit executives or create too many restrictions.

Here is what HR brings to the team:

- **Ensures the business complies with privacy laws**
- **Helps craft policies that are clear and effective**
- **Recommends third-party service providers**
- **Helps implement cybersecurity measures**
- **Drives awareness and better cyber manners**

A HOLISTIC PLAN →

The HR team needs to advocate for a holistic plan that protects executives and key personnel from a business perspective, without invading their privacy. The HR team brings knowledge about which key staff have access and need protection.

A holistic plan to safeguard executives includes:

PROTECTING THEIR PRIVACY

To truly protect executives, it is critical to have a strategy that removes personal information about executives from public websites, regularly performs dark web searches for exposed personal credentials, and provides them with identity theft protection.

PROTECTING THEIR HOMES

Executives' homes should receive penetration testing weekly and regular scans of their networks for malware, botnets, and other security issues.

PROTECTING THEIR DEVICES

Executives' personal devices, including cell phones, tablets and laptops, need to be protected with the same level of security as their corporate devices, both inside and outside corporate walls.

PROTECTING THEIR PEACE OF MIND

Executives shouldn't have to be constantly looking over their shoulder or feel the need to be their own personal cybersecurity expert. A solid executive protection program becomes a resource and a guide for executives.

A holistic plan considers many other factors— for example, all of the homes that the executive may frequent – including vacation homes. It may also include planning to protect family members and assistants who can be a conduit for criminals to gain access to private and sensitive data through their own digital habits and accounts.

Finally, the holistic plan should be orchestrated with a platform that encompasses all the above factors in one place to ensure service level agreements are met for both the company and the executive.

CONCLUSION →

CONCLUSION

Today, the boundary between the professional and personal sphere is vanishing.

The reputation and personal brand of executives is also a business asset. Executives and key personnel are vulnerable in their homes and personal lives. This represents a high risk to the business as cybercriminals increasingly target individuals in their homes and private lives, as a path to the corporate network. The business case for executive cybersecurity and privacy protection beyond the walls of the business is strong.

HR can bring their people and policy expertise to bear as a key stakeholder with the CISO and any third-party solution providers. We invite you to set up a meeting if you would like to discuss the services we provide to the enterprise. BlackCloak is a trusted partner who can deploy enterprise protection around your key staff in order to protect business assets and data. BlackCloak defends the business and its assets beyond the four walls, while providing concierge, white-glove service to executives and key personnel.

SOURCES:

1. **How HR Can Become a Cybersecurity Ninja**
   https://hrexecutive.com/how-hr-can-become-a-cybersecurity-ninja/

2. **M-Trends 2020 Report**
   https://content.fireeye.com/m-trends/rpt-m-trends-2020

3. **Cybercriminals Increasingly Target Top Executives**
   https://www.insurancejournal.com/news/international/2020/04/14/564766.htm

4. **2020 Data Breach Investigations Report**
   https://enterprise.verizon.com/resources/reports/dbir/

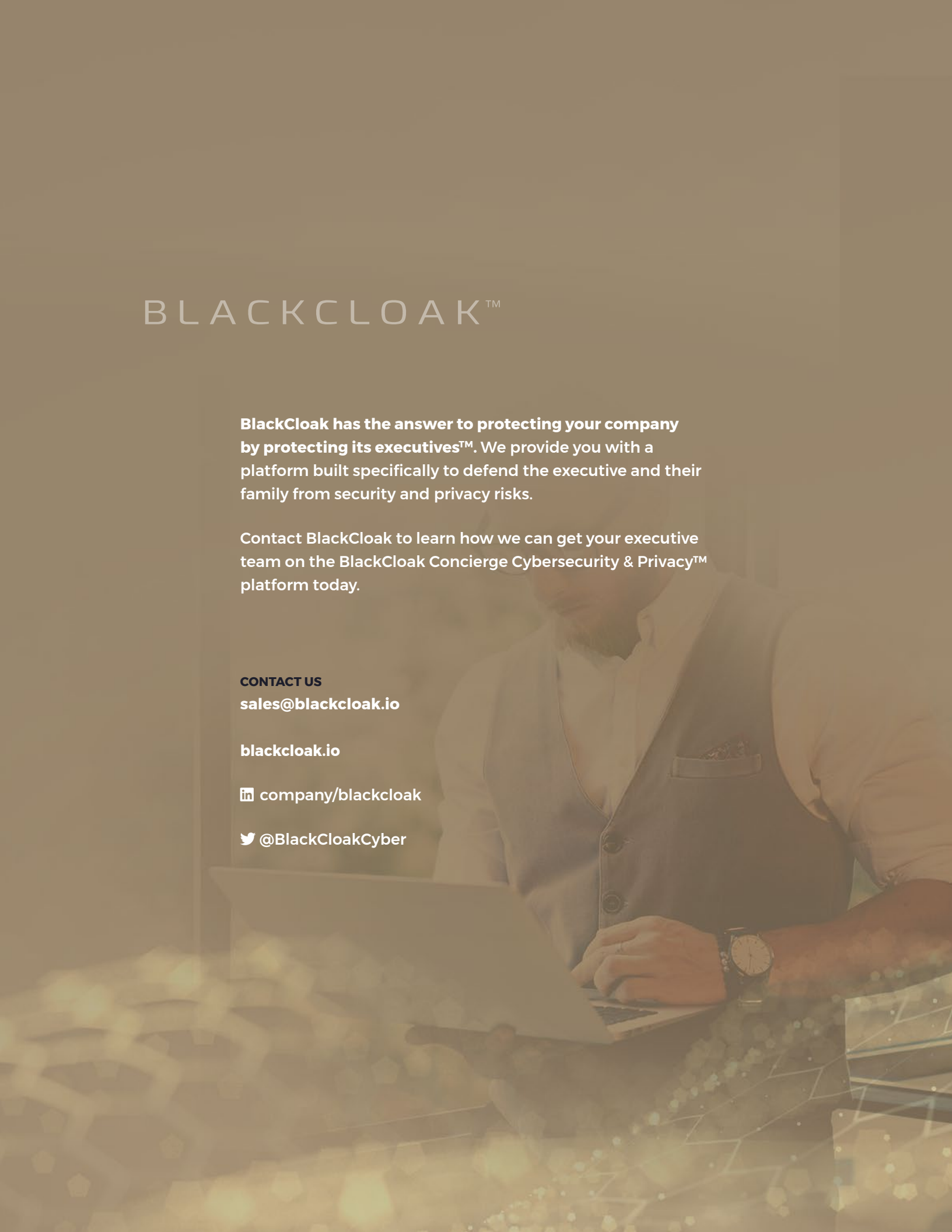
5. **Safeguarding your biggest cybersecurity target**
   https://www.cio.com/article/3247428/safeguarding-your-biggest-cybersecurity-target-executives.html

6. **The urgency to treat cybersecurity as a business decision**
   https://www.gartner.com/en/documents/3980891/the-urgency-to-treat-cybersecurity-as-a-business-decision

BLACKCLOAK™

BlackCloak has the answer to protecting your company by protecting its executives™. We provide you with a platform built specifically to defend the executive and their family from security and privacy risks.

Contact BlackCloak to learn how we can get your executive team on the BlackCloak Concierge Cybersecurity & Privacy™ platform today.



CONTACT US

sales@blackcloak.io

blackcloak.io

company/blackcloak

@BlackCloakCyber